REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-25 are pending in the application. The Examiner additionally stated that claims 1-25 are rejected. By this communication, claims 1, 9-10, 16, and 21 are amended. Hence, claims 1-25 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-25 under 35 U.S.C. 103(a) as being unpatentable over Kessler, US6789147 (hereinafter, "Kessler"), in view of Colavin, U.S. Publication No. 20040103263 (hereinafter, "Colavin"), and further in view of Miller, US6081884 (hereinafter, "Miller"). Applicant respectfully traverses the Examiner's rejections.

Claim 1 recites:

1. An apparatus for performing cryptographic operations, comprising:

    an x86-compabitle microprocessor, comprising:

        fetch logic, configured to receive a single, atomic cryptographic instruction, wherein said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation, and wherein said single, atomic cryptographic instruction prescribes one of a plurality of cryptographic algorithms;

        algorithm logic, operatively coupled to said single, atomic cryptographic instruction, configured to direct said x86-compatible microprocessor to execute said encryption operation according to said one of a plurality of cryptographic algorithms; and execution logic, operatively coupled to said algorithm logic, configured to execute said encryption operation, wherein said execution logic comprises:

a cryptography unit for executing a plurality of cryptographic rounds required to complete said encryption operation, wherein said cryptography unit executes a first plurality of micro instructions generated by translation of said single, atomic cryptographic instruction; and

an x86 integer unit, wherein said cryptography unit operates in parallel with said x86 integer unit to accomplish said encryption operation, and wherein said x86 integer unit executes a second plurality of micro instructions generated by translation of said single, atomic cryptographic instruction to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said encryption operation.

Nowhere does the cited art disclose **wherein said cryptography unit operates in parallel with said x86 integer unit to accomplish said encryption operation, and wherein said x86 integer unit executes a second plurality of micro instructions generated by translation of said single, atomic cryptographic instruction to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said encryption operation**, as is recited in claim 1. This limitation is disclosed in several places in the instant specification. For example, see paragraph [0056].

The Examiner argues that “Kessler discloses a co-processor that includes multiple execution units (FIGURE 2) wherein each of the execution units includes and execution queue to store cryptographic instructions received by the co-processor (Figure 8 & col. 4, lines 12-13)” and that “the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue (Figure 8 and col. 9, lines 7-43)." However, it is respectfully submitted that Kessler's security operation blocks 807, 809, 811, 813, 815, 819 are configured to specifically execute primitive security operations such as AES (block 807), 3DES (809), and ALU (block 815), for example. Yet, none of the cited references teach or suggest that a cryptography unit as recited in claim 1 operates *in parallel* with an x86 integer unit to perform a prescribed encryption operation, where the x86 integer unit executes **a second plurality of micro instructions generated by translation of said single, atomic cryptographic instruction to test a bit in a flags register, to update text pointer registers, and to process interrupts.** This is because the configuration of Kessler, Colavin, and Miller, as the Examiner suggests, does not contemplate performance of an encryption operation by an 86-compatible microprocessor, and would not as a consequence thereof consider how to perform this operation in the presence of normal x86 interrupts as would be incurred when operating under an operating system such as Windows or OSX. What the Examiner has suggested by combining these references is that it would be advantageous to integrate Kessler's co-processor into an x86-compatible microprocessor (in fact, the Examiner suggested the opposite, that of integrating an entire x86-compatible microprocessor into the co-processor of Kessler) because then cryptographic operations could be performed.

Applicant respectfully asserts that such a combination of references does not consider at all how a complex encryption operation can be accomplished by a general purpose CPU, such as an x86-compatible microprocessor. What happens when normal operating system interrupts occur? How are intermediate results preserved in the presence of interrupts? These issues are not even contemplated by the cited art. However, the present does contemplate that an x86 microprocessor will necessarily be performing other computation-intensive and interruptive tasks—in addition to the encryption operation—because the cryptographic rounds are performed by an integrated cryptography unit executing a first plurality of micro instruction, *while in parallel* an x86 integer unit is executing a second plurality of micro instructions to **test a bit in a flags register, to update text pointer registers, and to process interrupts.**

Furthermore, Applicant submits, yet again again, that the point that Colavin makes in the Abstract and paragraph [0018] is that *identical processing elements* in a coprocessor configured in parallel can be used to accelerate execution of portions of a program having high instruction level parallelism, which not germane to cryptographic operations due to the high data dependency requirements in sub-operations. Colavin does not teach or suggest a cryptography unit operating in parallel with an x86 integer unit, each performing *entirely different sub-operations* in order to accomplish an overall encryption operation.

Thus, for at least the above reasons, it is respectfully asserted that claim 1 is patentably distinct and non-obvious over the cited art. Consequently, it is requested that the rejection be withdrawn.

Claim 21 recites substantially the same limitations as have been argued above as being allowable over the combination of Kessler, Colavin, and Miller. Accordingly, it is requested that the rejection of claim 21 be withdrawn as well.

With respect to claims 2-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-15.

With respect to claims 22-25, these claims depend from claim 21 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 22-25.

As per claim 16, substantially the same limitations are recited as have been argued above with regard to claims 1 and 21, the exception being that claim 16 recites that the single atomic cryptographic instruction prescribes a decryption operation. Consequently, it is requested that the rejection be withdrawn since the recited limitations are not taught, contemplated, or suggested by the combination of Kessler, Colavin, and Miller.

With respect to claims 17-20, these claims depend from claim 16 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 16-20.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-25 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

By: /Richard K. Huffman/

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

Date: 06/24/2010